CHAPTER 5

RISK ASSESSMENTS

A. INTRODUCTION

1. The purpose of this chapter is to provide DoD managers guidance on assessing risks in automated information systems. While introducing efficiencies in governmental activities, automation simultaneously introduces new and different vulnerabilities. A risk assessment is conducted to determine susceptibility to waste, loss, and abuse.

2. Based on the results of risk assessment, an agency can proceed with its internal control evaluation, improvement and reporting process.

3. Under revised OMB Circular A-123, (reference (c]), agencies are required to make risk assessments to identify potential risks in agency operations that require corrective action or further investigation through internal control evaluations or other actions. These may follow the risk assessment procedures in the Internal Control Guidelines or may be based on a systematic review building on management's knowledge, information obtained from management reporting systems, previous risk assessments, audits, etc. Management should update its risk assessment of components at least once every 5 years and as major changes occur.

4. OMB Circular A-130, (references (e)) requires agencies to establish a level of security for information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information systems.

B. BASIC APPROACH

1. Internal controls should provide reasonable, although not necessarily absolute, assurance of minimal risks. Reasonable assurance recognizes that the costs of developing and instituting internal controls should not exceed the benefits derived from reducing risks. Risk assessment consists of four measures:

a. Analyzing the management control environment.

b. Evaluating general automated system controls.

c. Evaluating application controls.

d. Evaluating inherent risks associated with programs or functions supported by automated systems.

2. Questionnaires were developed to help managers gather and analyze information about the system's internal controls. The questionnaires are self-explanatory. Responses will be a simple "yes" or "no." Several "no" responses within one section may indicate control weaknesses, and depending on inherent risk, may indicate high vulnerability. However, judgment needs to be applied. For example, one "no" response to a critical question could indicate the need for a more detailed internal control review and the need for corrective action.

c. <u>QUESTIONNAIRE 1 - ANALYSIS OF THE MANAGEMENT CONTROL ENVIRONMENT</u>. Questionnaire 1 has been developed to assist in analyzing the management control environment in which automated operations or applications are conducted. First, management must assess the potential for waste, loss, mismanagement> unauthorized use, or misappropriation that exists in each automated operation or application. Second, management's control systems must be examined. To assess the management control environment, several factors should be considered, including:

- AIS Standards, Policies, and Procedures
- AIS Planning, Budgeting, and Reporting
- Prior Internal Audits and-Reviews, and Management's Responsiveness
- AIS Quality Assurance

1. <u>AIS Standards, Policies, and Procedures Considerations:</u> Implementing IRM policies and procedures should cite and be based on authorizing legislation, Departmental regulations, and Federal regulations concerning IRM, as appropriate. They should be updated to remain current. These policies and procedures must be promptly distributed to those who have internal control responsibilities and should include specific control guidance for AIS activities. "YES" answers to the following questions would indicate a low vulner-ability to risk.

<u>YES</u> <u>NO</u>

a. Has management initiated policies and proce-dures for timely implementation of DoDIRM standards? ___ ___

b. Are changes to existing policies and procedures disseminated promptly to all appropriate organizational units and individuals? ___ ___

YES NO

c. Have internal control and security objectives been defined in regard to automated operations and applications? ___ ___

d. Are specific internal controls, resource acquisition, system development and modification, and operating policies “ and procedures issued under these DoD standards? ___ ___

2. IRM Planning, Budgeting, and Reporting Considerations. Management's commitment to meeting goals concerning planning, budgeting, and reporting practices should reflect current Government policy and be widely publicized. Goals should include: (1) establishing budgeting policies; (2) adherence to these policies; and “(3) development and use of short- and long-range planning. “YES” answers to these questions reflect a low vulnerability to risk in this area.

YES NO

a. Does an Advisory Council exist, meet regularly, and is it chaired by a top management representative? ___ ___

b. Does the planning process include short- and long-range plans and clearly establish and document mission requirements, strategy, goals, and objectives? ___ ___

c. Does the planning process consider budgeting for financial, personnel, technical resources (e.g., hardware, software, communications and system interface) and compare and select among alternatives based upon quantified life-cycle costs, benefits and risk projections? ___ ___

d. Are plans usually followed? If not, are deviations from plans adequately documented with justification? ___ ___

e. Are plans and budgets for financial, personnel, and technical resources consistent with Departmental plans and budgets? ___ ___

3. Considerations Concerning Prior Internal Audits and Reviews and Management's Responsiveness. The assessment of an AIS vulnerability may be supported by reviews or audits by Internal Audit (the Inspector General where that organization exists), the U.S. General Accounting Office, or congressional committees. The primary considerations in this area are the corrective actions identified and management's response to them, "YES" responses to the following questions indicate low vulnerability.

YES NO

a. Does the Internal Audit function perform audits of operational systems, systems under development, and other activities addressing general. and application controls? ___ ___

b. Are corrective actions identified as a result of audits or reviews of the automated operation or application? ___ ___

c. Are there no significant audit or review findings that represent continuance of **previously** identified **problems?** ___ ___

4. AIS Quality Assurance Considerations. Quality assurance **is** a critical function in the automated information systems environment to ensure user departments are satisfied with the quality of information systems. Quality assurance should be responsible for reviewing **all** aspects of information systems to ensure adherence to the standards and implementing policies and procedures. In addition, the quality assurance function should be responsible for ensuring the accuracy and reliability of automated systems' outputs. "YES" answers to the following questions indicate low vulnerability to risk in the area.

YES NO

a. Has a quality assurance function been established to determine if user departments are satisfied with the quality of automated systems and tested internal controls incorporated in the information systems? ___ ___

b. Is the quality assurance function ***responsible for reviewing all aspects*** of automated systems to ensure adherence to standards, policies and procedures? ___ ___

YES NO

c* Does the quality assurance function monitor the accuracy and reliability of automated systems' outputs? ___ ___

D. QUESTIONNAIRE 2 - EVALUATION OF GENERAL SYSTEMS CONTROLS. This questionnaire helps to determine if general systems controls are in place to prevent or minimize waste, loss, mismanagement, unauthorized use, or misappropriation. The level of comprehensiveness and intensity of review depends on the size of the system, including hardware and software. This questionnaire focuses on the following aspects of automated general control:

- Organizational Checks and Balances.
- Data Center Operations.
- Security and Control.
- Environmental Protection and Disaster Recovery and/or Contingency Planning.
- System Design, Development, and Modification Control.
- System Software Control.
- Distributed Processing and Network Operations Control.
- Personnel.
- Microcomputer Control.

1. Organizational Checks and Balances Considerations. Effective internal controls need to be established over the data processing operations and applications because of the concentration of functions brought about by the computer. "YES" responses to the following questions indicate low vulnerability to risk in this area.

YES NO

a. Are duties separated to ensure no individual performs more than one of the following functions;

(1) Originating Data. ___ ___

(2) Processing Data. ___ ___

(3) Distributing Data. ___ ___

(4) Inputting Data. ___ ___

YES NO

(5) Reviewing Data. ___ ___

b. Are duties separated among computer operations, systems development, systems programming, applications programming, and data control? ___ ___

c. Are duties and separation requirements documented and enforced? ___ ___

2. Data Center Operations Considerations: Control procedures for data center operations should be established and followed to ensure accuracy and completeness of the information maintained and processed by the DoD data centers. "YES" responses to the following questions indicate low vulnerability to risk in this area.

YES NO

a. Does a formal production schedule exist to ensure that resources are effectively used and that the needs of users are met?

b. Is a formal control group established within the data center to monitor both decentralized and centralized job entry? ___ ___

c. Does a schedule exist for preventive maintenance according to established site and vendor procedures? ___ ___

d. Are formal malfunction reporting procedures established, documented, and enforced? ___ ___

e. Are procedures for user billing and charge-back documented and are such procedures tied into a job accounting system for the data center's resources? ___ ___

f. Do detailed written operator instructions (including set-up, file disposition, error response and restart and/or recovery) exist and are they followed? ___

YES NO

g. Are supervision and review of operations sufficient to provide reasonable assurance that the computer is used only for authorized purposes and that operators are following prescribed procedures? ___ ___

3. Security and Control Considerations: Control and/or procedures consistent with DoDD Directive 5200.28 and OMB Circular A-130 references (r) and (e)), for computer security should be established and followed to safeguard ADP resources. The hardware, software, and data are all assets that should be protected against theft, loss, unauthorized manipulation, fraudulent activities, and natural disasters. To minimize these risks, controls to limit access to the data center, decentralized hardware including microcomputers, system and application programs, system documentation and output should be established. "YES" responses to the following questions indicate low vulnerability to risk in this area.

YES NO

a. Is responsibility for computer security at the site established, documented, and assigned? ___ ___

b. Are required controls in place to protect national security information? ___ ___

c. Are clearly defined security policies and procedures-established and enforced? ___ ___

d. Are risk analyses performed according to a specific timetable? ___ ___

e. Are personnel security policies for screening employees and contractor and/or service personnel documented and enforced? ___ ___

f. Is access to the computer area by individuals in need of limited access (e.g., hardware manufacturer, custodial personnel, etc.) supervised and controlled? ___ ___

g. Are procedures limiting access to critical forms, such as identification cards, checks , and source documents, documented and enforced? ___ ___

YES NO

h. Are user identification codes and passwords used to validate users of the system, data and software? . ___ ___

i. (1) Is separate computer access control and/or security software utilized? ___ ___

(2) Does it control access to individual data files and elements, application programs, and other system software? ___ ___

(3) Are accesses to the system recorded (either manually or automatically)? ___ ___

4. Environmental Protection and Disaster Recovery and/or Contingency Planning Considerations: Procedures should be established to help protect critical files, programs, and system documentation from fire or other natural disasters. These procedures should be formally documented and periodically updated and tested. They should contain the detailed steps computer operations personnel should take in the event of an emergency. The data center should be equipped with both smoke and fire detection devices. Floors, walls, ceilings, and draperies should be made of noncombustible material. Alternate power sources or other electrical backup devices should be installed to limit the impact of a power shortage or blackout. Formal backup arrangements should also be established with another compatible data center. Copies of critical files, programs, and documentation should be stored at an off-site location. Steps should be taken to make sure that the off-site materials are periodically updated and that the backup center has sufficient capacity to process the additional work load. Periodic tests of the backup arrangements should also be performed.

YES NO

a. Have emergency disaster recovery and/or contingency planning procedures been documented and are they up-to-date? ___ ___

b. Do they include steps to take in the event of a natural disaster by fire, water damage, etc. , and intentional damage by sabotage, mob action, bomb threats, etc? ___ ___

c. Are employees familiar with the emergency procedures? ___ ___

YES NO

d Is the data center separated from adjacent areas by fire resistant partitions, walls, etc.? ___ ___

e. Are noncombustible floors, ceiling, and/or draperies used in the data center? ___ ___

f. Are any activities conducted adjacent to the data center that might endanger it by flood, fire, or explosion? ___ ___

g. Are heat and smoke detectors installed in the following areas:

In the ceiling? ___ ___

Under raised floors? ___ ___

In the air return ducts? ___ ___

h. Are battery-powered emergency lights placed in strategic locations to assist in evacuation should power be interrupted? ___

i. Is the data center protected by an automatic fire-suppressing system? ___ ___

j. Is the data center equipped with temperature and humidity gauges that automatically acti-vate signals if either exceeds the normal range? ___ ___

k. Is the data center backed up by an uninterruptable power source system? ___ ___

1. Are there provisions for retaining and/or copying master files and a practical means of reconstructing a damaged or destroyed file? ___

m. Are sufficient generations of files maintained to facilitate reconstruction of records? ___ ___

n. Are duplicate copies of data files application programs, system software, and critical documentation kept and updated periodically ata remote location and restricted from unauthorized access? ___

YES NO

o. Is there backup capability at an off-site location? ___ ___

p" Have critical locations been provided with adequate terminals, modems, and communications lines? ___ ___

q. Are operations procedures periodically tested at the backup data center? ___ ___

5. Application Design, Development, and Modification Control Considerations. Systems design, development, and modification process should provide adequate separation of duties and assure user, management, and internal audit participation. Additional key elements are documentation, computer program testing, system acceptance testing, and computer program change control procedures. The age and life expectancy of an application or operation will determine to some degree its susceptibility to fraud, waste, loss, unauthorized use, or misappropriation. "YES" responses to the following questions indicate low vulnerability to risk in this area.

YES NO

a. Is the application development predicated on a system development life-cycle methodology? ___

b. Are formal, standard control practices followed in system design and development and are they reviewed for proper implementation? ___ ___

c. Are systems documented as they are being designed? ___ ___

d. Are new or modified programs and/or systemssubjected to comprehensive testing (both computer program and user acceptance) prior to implementation? ___ ___

e. Are test results approved by user departments and AIS management prior to conversion to a new system? ___ ___

f. Are system development, pre-implementation and post-implementation reviews of an entire (manual and automated) system performed? ___ ___

YES NO

g. Are procedures in place that define who can initiate a system change request and who can authorize a change? ___ ___

h. Is a log kept of completed system changes and changes in process? ___ ___

i. Is the application or operation using up-to-date techniques and being maintained by people familiar with the techniques? ___ ___

j. Is the application stable or undergoing only minor-or well-controlled enhancements? ___ ___

6. Systems Software Control Considerations. System software purchased from vendors is normally reliable and includes built-in error checking features capable of detecting any processing errors it might cause. However, through program changes and software options, systems software support personnel control many details of computer operations and application processing. "YES" responses to the following question indicate low vulnerability in this area.

YES NO

a. Are modifications to system software authorized and approved by ADP management before changes are made? ___

b. Is access to system software and related documentation restricted to authorized personnel? ___ ___

c. Are procedures established, documented and enforced to provide assurance that systems software changes are thoroughly and independently tested and properly implemented? ___

7. Distributed Processing and Network Operations Control Considerations. Control procedures for distributed processing and network operations should be formally established and followed. With the rapid increase of decentralization of systems, control and integrity have become major concerns. "YES" answers the following questions indicate low vulnerability in this area.

YES NO

a. Are standards and policies for general network control clearly established and followed? ___ ___

b. Does a network policy exist requiring audit trails and backup of all network communications activity for both network messages and applications-processed data? ___ ___

c. Do distributed processing and network hardware controls include memory protection, alternate communications routing, communication protocols and timely failure and/or recovery mechanisms? ___ ___

d. Are local and consolidated network p erformance reports prepared to regularly “ convey key elements, such as network s ystems availability, performance to schedules, response times, processing efficiencies, and performance problems? ___ ___

e. Are local and/or private communications lines and switches secured and accessible only by authorized personnel? ___ ___

f. Are communications security methods used toprotect transmission of sensitive and/ornational security information? ___ ___

8. Personnel Considerations. Important factors in this area are the integrity and competency of contractor and agency personnel assignedto carry out AIS operations and applications activities. Personnel must have adequate experience and training to be competent. “YES” answers to the following questions indicate low vulnerability to risk in this area.

YES NO

(1) Are appropriate security clearances granted prior to allowing personnel access to sensitive or national security information? ___ ___

(2) Do key personnel receive adequate training in the professional, technical, internal control and security aspect of their jobs? ___ ___

YES NO

(3) Are employees regularly informed of new policies and procedures including internal management control requirements? ___ ___

9. Specific Microcomputer Control Cons iderat ions. Control procedures for microcomputer operations should be established and followed to ensure the proper management and use of microcomputers and the accuracy of the processed data. Implementing certain control procedures unique to microcomputers should decrease the risk of illegal system access, data loss, and stolen hardware. “YES” responses to the following questions indicate low vulnerability to risk in this area.

YES NO

a. (1)Have policies and procedures regarding the acquisition and use of microcomputer resources been developed? ___ ___

(2)-Are policies regarding the acquisition and use of microcomputer resources adhered to and enforced? ___ ___

(3)Do policies prohibit the use of copyrighted and/or unauthorized software that the activity has not leased or purchased? ___ ___

b. Are the functions and capabilities of microcomputer based systems document ed? ___ ___

c* Are microcomputer resources inventories, hardware and software, maintained in a central location and verified periodically? ___ ___

d. Do adequate controls exist to ensure that microcomputer hardware is not stolen or vandalized? ___ ___

e. Are guidelines followed for the backup of programs and files , and for their safe-keeping? ___ ___

f. Are labeling and storage procedures for sensitive information, storage media and microcomputers established? ___ ___

E. QUESTIONNAIRE 3 - EVALUATION OF APPLICATION CONTROLS

This questionnaire helps to determine if appropriate application controls are in place. Users of automated information systems have primary responsibility for assuring their systems have adequate controls, including security. Users should establish the sensitivity or the risk and magnitude of loss or harm that could result from improper operation of their application. Appropriate administrative, physical, and technical controls should be implemented by users. This questionnaire is intended to be used when reviewing functional controls of agency activities that use ADP to support their activities. It focuses on the following aspects of automated application control:

- Purpose and Characteristics.
- Assuming the Risk at the Data Center.
- Data Origination.
- Data Input.
- Data Processing.
- Data Output.

1. Purpose and Characteristics Considerations: The purpose and characteristics of the ADP application should be evaluated by its user to determine the degree to which it is susceptible to waste, loss, unauthorized use, mismanagement , or misappropriation. For example, ADP applications that maintain or process classified or sensitive data that may (1) have a significant impact outside the department or agency; (2) cause transfers of property or receipt and/or payment of money; or (3) involve approvals or granting of authority that are sensitive and, thus, particularly vulnerable. "YES" answers to the following questions indicate low vulnerability.

YES **NO**

a. Have the users made a clear determination of the sensitivity of each application and the information processed? ___ ___

b. Is that determination based on the total risk and magnitude of loss or harm that could result from improper operation of the application or disclosure of information? ___

YES NO

c* Where the application is considered sensitive, has the user:

(1) Participated in defining and approving security specifications for the application? ___ ___

(2) Verified that security controls are working and have been certified as operationally adequate for the application? ___ ___

(3) Reviewed and recertified the application in the last 3 years? ___ ___

(4) Assured that security or other control weaknesses have been corrected? ___ ___

[5) Included security or other control weaknesses found in their annual report? ___ ___

(6) Assured that procedures are in place that control who can initiate a change and who can authorize a change? ___ ___

2. Assuming the Risk at the Data Center: Since users of ADP have ultimate responsibility for the security and integrity of their application, they assume the level of risk at the installation that processes their application. It is critical, therefore, that they have the ability to reduce that risk to an acceptable level [even if required to go to a different installation for processing). "YES" responses to the following questions indicate low- vulnerability in this area.

YES NO

a. Does the user organization understand the level of risk at the installation where his or her application is processed? ___ ___

b. Is the user organization apprised of changes at the installation that may impact that level of risk? ___ ___

c. Does the user understand the vulnerability of the communication lines and links. used in the application? ___ ___

YES NO

d. Does the user know who is responsible for security at the installation where his or her application is processed? ___ ___

e. Is the user organization free to seek data processing support at a different installation? ___ ___

f. Is the user familiar with the disaster recovery and backup plan at the data processing installation where his or her application is processed? ___ ___

g. Does the user have a contingency plan consistent with the disaster recovery and backup plan for essential functions? ___ ___

h. If a data base management system is used in the users’ application, does he or she understand its vulnerabilities and special control considerations? ___ ___

i. Does the user have secutity measures in placeto protect ADP equipment, such as microcomputers and remote terminals in his or her area? ___ ___

3. Data Origination Considerations: Data origination controls are used to ensure the accuracy, completeness, and timeliness of data prior to its being converted into a machine-readable format and entered into the computer application. Controls should ensure that the data reaches the computer application without loss, unauthorized addition, modification, or error. “YES” responses to the following questions indicate low vulnerability to risk in this area.

YES NO

a. Do documented procedures exist to explain methods for proper source document origination, authorization, data collection, input preparation, error handling, and retention? ___ ___

b. Are duties appropriately segmented for originating data, inputting data, processing data, distributing output, and reviewing output? ___ ___

c. Are signatures required to approve all transactions? ___ ___

YES NO

d. Are source documents accounted for? ___ ___

e. Is access to source documents, blank input forms, and copies. of source documents restricted only to authorized personnel? ___ ___

f. Do documented procedures exist to explain the methods for source document error detection, correction, and reentry? ___ ___

4. <u>Data Input considerations:</u> Data input controls ensure the accuracy, completeness, and timeliness of data during its conversion into machine-readable form and entry into the application. Data can be input through either on-line or batch processinq. "YES" responses to the following questions “indicate low vulnerability to risk in this area.

YES NO

a. Are procedures established for the conversionand entry of data to ensure separation of duties as well as routine verification of work performed in the data input process? ___ ___

b. Are procedures related to the conversion and entry of data through terminals, such as the use of passwords, followed to deter unauthorized use? ___ ___

c. Do documented procedures exist to explain the process of identifying, correcting, and reprocessing data rejected by the application? ___ ___

d. Is input data validated and edited close to the point of origin to ensure the application rejects any incorrect transaction before its entry into the system? ___ ___

e. Is all data that does not meet edit requirements rejected from future processing, reflected on an error message, and written to a suspense file? ___ ___

f. Are error-handling procedures in place to facilitate the timely and accurate resubmission for processing of all corrected input data?

YES NO

g. Are change commands, rather than delete or erase commands, used to correct errors on the suspense file? ___ ___

h. Are personnel with access to the system appropriately screened? ___ ___

i. Are personnel granted access to only those resources and information required for their duties and no more? ___ ___

j. Are personnel restricted from bypassing and overriding validation and editing problems? ___ ___

k. Have personnel received security awareness training apprising them of the vulnerabilities of the application and techniques for enhancing security? ___ ___

1. Is authorization of access (user identification, passwords, etc.) to the application actively managed by the user? ___ ___

m. Is the identity of users verified prior to system access? ___ ___

5. Data Processing Considerations. Data processing controls are used to ensure the accuracy, completeness, and timeliness of data during processing by the computer. "YES" responses to the following questions indicate low vulnerability to risk this area.

YES NO

a. Does the data center maintain a schedule showing when each application is to be run and needs to be completed? ___ ___

b. Are computer-generated control totals (run-to-run totals) reconciled to check for com-pleteness of processing? ___ ___

c. Do error-handling procedures identify erroneous transactions without processing them and without undue disruptions to the processing of other valid transactions? ___ ___

d. Is operator intervention of data processing restricted? ___ ___

	YES	NO
e. Is relationship editing performed between the input transaction and master files to check for appropriateness and correctness prior to updating?	___	___
f. Are there procedures for controllinq the release of ADP storage media that have contained sensitive or classified information?	___	___

6. <u>Data Output Considerations:</u> Data output controls are used to ensure the integrity of output and the correct and timely distribution of outputs produced. Not only should outputs be accurate but they must be timely. Data can be output either by on-line or batch processing. "YES" responses to the following questions indicate low vulnerability to-risk in "this area.

	YES	NO
a. Are output reports reviewed for completenessand form?	___	___
b. Are outputs balanced to control totals withaudit trails available to facilitate tracing and reconciliation?	___	___
c. Are outputs controlled in accordance with written instructions?	___	___
d. Are outputs marked by appropriate security classification?	___	___
e. Are outputs marked in accordance with the level of sensitivity of the information?	___	___
f. Are procedures followed to report and control errors contained in output?	___	___
g. Does the user periodically verify the accuracy of all outputs?	___	___
h. Are appropriate methods used to dispose of documents that are not needed?	___	___
i. Are personnel with access to the output appropriately screened?	___	___

YES NO

j. Have personnel handling the output received security awareness training apprising them of the vulnerability of the application? ___ ___

F. QUESTIONNAIRE 4 - ASSESSMENT OF INHERENT RISK. Questionnaire 4 was developed to help assess inherent risk. Analysis of each identified automated system must be performed to assess the potential for waste, loss, unauthorized use, or misappropriation due to the nature of the program itself. Matters to be included in the analysis are:

. Purpose and characteristics.

● Value of resources.

. Impact outside the agency.

. Age and life expectancy.

. Degree of centralization.

● Special concerns.

1. Purpose and Characteristics Considerations. The purpose and characteristics of the program being supported by the ADP operation or application should be considered to determine the degree to which it is susceptible to waste, loss, unauthorized use, mismanagement, or misappropriation. "YES" answers to the following questions indicate high vulnerability in this area.

YES NO

a. Is the program subject to:

(1) Broad or vague legislative authority or regulations? ___ ___

(2) Cumbersome legislative or regulatory requirements?' ___ ___

(3) Broad or vague missions, goals, or objective? ___ ___

b. Is work assigned that often includes interaction with organizations outside management s' chain of command? ___ ___

c. Do contractors perform work that could be considered Government work (e.g., a Government-owned project operated by a contractor) ? ___ ___

YES **NO**

d. Does the program involve handling classified or sensitive information? ___ ___

e. Does the program involve handling valuable or sensitive inventory items or cash receipts or documents that can be used instead of cash? ___ ___

2. Value of Resources Considerations. Programs or functions that require a large budget to operate and/or control or that disperse items of high value are more susceptible than lower budget programs to waste, loss, unauthorized use, or misappropriation. A “NO” answer to the following question indicates low vulnerability to risk in this area.

YES **NO**

a. Does the program require a large budget” to operate and/or does it control or disburse items of high value? Items to be included: ___ ___

(1) The annual operational cost (including salaries, hardware, software, etc.). ___ ___

(2) The value of the items controlled (including data, property, funds, etc.). ___ ___

(3) Value of the data supporting the program (costly to acquire or replace, highly valuable to outside sources, etc.). ___ ___

3. Impact Outside the Program. If a program or function has a significant impact outside the activity, it may be subject to pressures to circumvent internal controls. A “NO” answer to the following question indicates low vulnerability in this area.

YES **NO**

a. Does the program or function have a significant impact outside the activity? Items to be considered include: ___ ___

(1) The number of citizens impacted by the program. ___ ___

(2) The impact on economic well-being of outside individuals or groups. ___ ___

YES NO

(3) Impact on the health of outside individuals or groups. ___ ___

(4) Impact on the safety of outside individuals or groups. ___ ___

4. Age and Life Expectancy Considerations: The age and life expectancy of a program are factors to consider when analyzing risk. New or changing programs may lack written policies or procedures; lack adequate resources; have inexperienced managers and personnel; or lack devices to measure performance. Programs that are phasing out may lack adequate resources or involve close-out activities for which controls have not been developed, or involve accounting for significant amounts of money or other resources. "YES" answers to the following questions indicate low vulnerability in this area.

YES NO

a. Is the program in existence less than 2 years? ___ ___

b. Is the program undergoing substantial modification or reorganization? ___ ___

c. Will the program be eliminated within 2 years? ___ ___

5. Degree of Centralization Considerations. The extent to which a program or function is operated in a centralized or decentralized manner should be determined. Excessive centralization of a program or function can increase the likelihood of loss due to fraud, waste, abuse, or mismanagement. "YES" ***responses*** to the following questions indicate low vulnerability to risk in this area:

YES NO

a. Is the program managed and controlled on a day-to-day basis? Factors to be considered include: ___ ___

(1) Centralization (i.e., the program is managed and controlled on a day-to-day basis by Headquarters organizations or staff.) ___ ___

(2) Decentralization (i.e., the program is managed and controlled on a day-to-day basis by field i nstallations or staff.) ___ ___

<u>YES</u> <u>NO</u>

(3) Contractor administration (i.e. , the program is managed and controlled on a day-to-day basis by a **non-DoD** organization.) ___ ___

(4) Other (i. e., the program is managed and controlled by some combination of the above or by other means.) ___ ___

6. <u>Special Concerns</u>. Often, the existence of special concerns for an activity may be indicative that for some reason it is highly susceptible to waste, loss, unauthorized use, or misappropriation, and should be treated as such. Consideration should be given as to whether the program or function has been the focus of **special** attention. "YES" responses to the following questions indicate low vulnerability to risk in this area.

<u>YES</u> <u>NO</u>

a. Has special interest in the program been exhibited by top executive officials, Congress, special interest groups or lobbyists? ___ ___

b. Has the program received particular attention from the media? ___ ___

c. Has the program been subject to recent litigation? ___ ___

G. <u>WLNERABILITY ASSESSMENT USING THE RESULTS</u>.

1. The results of risk assessment questionnaires are used to:

a. Support management **judgment** as to the degree of risk involved,

b. Report weaknesses, and

c. Determine if more rigorous evaluation is needed.

2. Not all weaknesses are material in nature. In determining risk levels and in deciding on next steps, material weaknesses must be carefully considered in each agency' s Management Control Plan. These Plans are required for each agency by 1987 in accordance with OMB Circular A-123 (reference (c)) . Material weaknesses, if discovered, must also be included in prescribed annual reports to the President and Congress.

3. A material weakness is defined in reference (c) and the Internal Control Evaluation Guidelines as a situation in which the designed procedures or the degree of operational compliance, therewith, does not provide reasonable assurance that the objectives are being accomplished. The material weaknesses identified in the annual report should be of significance to warrant the attention of the President and Congress.

4. In the annual report to the President and Congress, the head of each agency must state whether the agency's systems comply with the Comptroller General's standards and must provide reasonable assurance that the objectives of internal control were achieved.